Update of Network Time Security for the Network Time Protocol

draft-ietf-ntp-using-nts-for-ntp-12

Daniel Franke, Dieter Sibold, Kristof Teichel

Changes from -11 to -12

- Changes due to IETF 101 Hackathon
  - Update of the time exchange diagram
  - Section 6. Protocol details:
    New language to make clear that cookies send from the server to the clients are encapsulated within the the NTS Authenticator and Encrypted Extensions extension
- Other Changes
  - Definitive statements about applicability to TLS 1.3
  - New language describing the padding within the 'Authenticator and Encrypted Extension Fields extension field'

Changes from -11 to -12

- Additions
  - Section 9 “Implementation Status”
    - Results from IETF 101 Hackathon
  - Within Section 4: NTS Key Exchange Length Limitations
    - Servers MUST accept request of at least 1024 octets
    - Clients SHOULD accept responses of at least 65536 octets

Next steps

- Consideration of **draft-dansarie-nts-00**
- WGLC